Richard C. Fipphen
Senior Counsel
WorldCom, Inc.
200 Park Avenue, 6th floor
New York, NY 10166
212 519 4867
Fax 212 519 4569
Richard.Fipphen@wcom.com

March 28, 2003

BY E-MAIL AND OVERNIGHT DELIVERY

Mary L. Cottrell, Secretary
Department of Telecommunications and Energy
One South Station, 2nd Floor
Boston, MA 02110

Re: DTE 99-271 - Performance Assurance Plan – Service Waiver Request

Dear Ms. Cottrell:

On March 18, 2003, Verizon Massachusetts ("Verizon") filed a petition with the Department seeking approval of its request for waiver of certain service quality results under the Performance Assurance Plan ("PAP" or "the Plan") for the month of January 2003. For the reasons discussed below, WorldCom opposes Verizon's waiver request and urges the Department to deny it.

The PAP, which became effective with Verizon's entry into the long distance market in Massachusetts, comprises performance measures and remedies designed to assure the company's provision of wholesale service to its competitors on a just and reasonable basis. To this end, the Plan plays a critical role in providing Verizon with incentives to meet and sustain performance standards that are essential to the continued development and availability of meaningful local competition in Massachusetts. Verizon's failure to meet any or all of the PAP's performance measures not only impedes the ability of competitors to provide service to their customers, but also threatens the very ability of competitors to continue doing business in the state. It is with these important considerations in mind that Verizon's waiver request should be evaluated.

Specifically at issue here is Verizon's request that its performance results in January 2003 be waived for three PAP pre-order measures with absolute standards (the "Pre-Order

Measures").[1] In support, Verizon contends that: (1) during the weekend of January 25, 2003, certain systems it uses were subject to an Internet computer attack by the Slammer Worm, a "self-propagating malicious code that exploits vulnerabilities in Microsoft SQL Server 2000, and certain other Microsoft products[;]"[2] (2) this event was beyond its control and occurred without warning; and (3) the Slammer Worm attack negatively affected its ability to satisfy the three Pre-Order Measures; and (4) it acted reasonably and prudently under the circumstances, consistent with industry practices in operating and protecting its cyber facilities, adding that patch management to prevent worms from infecting systems is an "extremely complex task."[3] Because of the impact the Slammer Worm had on its systems, Verizon proposes that the affected day - January 25th - be excluded from the calculation of the three Pre-Order Measures for the January 2003 performance month. If granted, the requested waiver would eliminate the monthly rebates due to CLECs in Massachusetts, approximately $164,000.

Given the gravity of the PAP to market competitors and end users alike, as well as the potential substantial reduction in rebates owed to CLECs for the month of January 2003, Verizon's waiver request warrants the utmost scrutiny. When subjected to that scrutiny, it becomes clear that Verizon's waiver request should be denied. As specified in the PAP, Verizon may file a petition for waiver to have its service quality results modified due to situations beyond its control that negatively affect its ability to satisfy only those measures with absolute standards. Among other things, that petition "must demonstrate clearly and convincingly the extraordinary nature of the circumstances involved."[4] Verizon has simply failed to make that requisite showing.

As an initial matter, as a company with its own network and systems over which it keeps vigilant watch, WorldCom appreciates the complexities involved in network and systems security. That said, the Slammer Worm attack at issue here was, in fact, a foreseeable event and not an extraordinary event beyond Verizon's control. This is because as early as June 24, 2002, Microsoft had issued a security bulletin (Bulletin MS02-039) to its customers notifying them of vulnerabilities in its Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 products that, if exploited, could impact customers' systems. That Bulletin was also widely distributed by other security alerting services that proactively notify their clients of network/systems vulnerabilities and impending cyber attacks.

Importantly, Bulletin MS02-039 not only explained the vulnerabilities in its Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 products and how to prevent

[1] Verizon requests waiver of the results for: (1) PO-2-02-6020 "OSS Interface Availability -Prime -EDI;" (2) PO-2-02-6030 "OSS Interface Availability - Prime - Corba"; and (3) PO-2-02-6080 "OSS Interface Availability - Prime - Web GUI."
[2] VZ Petition at 2.
[3] *Id.* at 11.
[4] VZ NY PAP at 18.

them from being exploited, recommending the use of Patch 056, but also rated the severity of the vulnerabilities as "critical." Microsoft's "critical" rating of the vulnerabilities ultimately exploited by the Slammer Worm is significant. Microsoft employs a security bulletin severity rating system to help customers decide which patches they should apply to avoid impact under their particular circumstances and how rapidly they need to take action. Since the severity rating system rates vulnerabilities as "low," "moderate," "important" and "critical," clearly the vulnerabilities rated "critical" are of the utmost concern and require the most immediate attention, *i.e.*, the timely application of patches.

The difficulties of patch management notwithstanding, at the very least, Verizon could be - and should be - reasonably expected to keep abreast of critical vulnerabilities and to defend its network and systems against them. While the Slammer Worm attack itself was beyond Verizon's control, protecting its systems was not. To this point, nowhere in its petition does Verizon assert that it did not have notice of the vulnerabilities to its systems. Furthermore, the fact that other large businesses, like WorldCom, were able to defend their systems against the Slammer Worm belies Verizon's suggestion that it could not do the same. Verizon should have applied the recommended patches that would have prevented the Slammer Worm from infecting its systems. Having failed to do so and thereby protect its systems against a preventable event, Verizon cannot be found to have acted in a reasonable and prudent manner. To find otherwise would inappropriately sanction an extremely liberal definition of "extraordinary" circumstances "beyond Verizon MA's control" on which grounds for a waiver of PAP results may be based. It would also force CLECs to pay the price for Verizon's failure to prevent vulnerabilities to its systems from being exploited by the Slammer Worm. Verizon and not CLECs should be held accountable for that failure.

Accordingly, for the reasons discussed here, the Department should deny Verizon's waiver request.

Respectfully submitted,

Richard C. Fipphen

Copies: Service List